UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

CELLULAR TELEPHONE ASSIGNED CALL NUMBER 937-554-7700

Case No. 3:21-MJ-45

Elizabeth Preston Deavers

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
SEE ATTACHMENT C	

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days *(give exact ending date if more than 30 days:* ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Go to Meeting *(specify reliable electronic means)*.

Date: February 4, 2021

Elizabeth Preston Deavers

Judge's signature

City and state: Columbus, OH

Elizabeth A. Preston Deavers, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **937-554-7700** (the "Target Cell Phone"), whose service provider is Verizon, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey, 07921.

2. Information about the location of the Target Cell Phone that is within the possession, custody, or control of Verizon including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to be Seized

All information about the location of the Target Cell Phone described in Attachment A for a period of thirty days, during all times of day and night. "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, Range-to-Tower (RTT) data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of Verizon, Verizon is required to disclose the Location Information to the government. In addition, Verizon must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Verizon's services, including by initiating a signal to determine the location of the Target Cell Phone on Verizon's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Verizon for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

ATTACHMENT C

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
21 U.S.C. §844	Possession of Controlled Substances

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE CELLULAR TELEPHONE ASSIGNED CALL NUMBER 937-554-7700	Case No. 3:21-mj-45 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

INTRODUCTION

1. I make this Affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **937-554-7700** (the "**TARGET CELL PHONE**"), whose service provider is Verizon, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey, 07921. The **TARGET CELL PHONE** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

3. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography and access with the intent to view child pornography; violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive and distribute child pornography through interstate commerce; and 21 U.S.C. § 844, which makes it a crime to possess controlled substances, have been committed, are being committed, and will be committed by WILLIAM SYDNEY HITCHINGS V (hereinafter referred to as "HITCHINGS"). There is also probable cause to believe that the location information described in Attachment B will

constitute evidence of these criminal violations and will lead to the identification of the locations where computer devices are utilized in the commission of the offenses.

PERTINENT FEDERAL CRIMINAL STATUTES

5. 18 U.S.C. § 2252(a)(2) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

6. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. 21 U.S.C. § 844 states that it is a violation for any person to knowingly or intentionally possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, from a practitioner, while acting in the course of his professional practice, or except as otherwise authorized by this subchapter or subchapter II of this chapter.

BACKGROUND INFORMATION

Definitions

10. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. **"Child Pornography"** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. **"Minor"** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. **"Sexually explicit conduct"** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. **"Internet Service Providers"** or **"ISPs"** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An **"Internet Protocol address"**, also referred to as an **"IP address"**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard.

Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. **"Hyperlink"** (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

h. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

i. **"Social Media"** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users' account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

j. **"Exchangeable image file format"**, also referred to as **"EXIF data"**, is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners, and other systems handling image and sound files stored by digital cameras. Most new digital cameras use the EXIF annotation, storing information on images such as shutter speed, exposure compensation, F number, metering system used, if a flash was used, ISO number, date and time the image was taken, etc.

k. **"Metadata"** is data that provides information about other data. For computer files, metadata can be stored within the file itself or elsewhere. Metadata for computer files includes the file name, the file type, where it is stored (*i.e.*, the file path), when it was created, when it was last modified and accessed, the file size, and other information.

l. **"Uniform Resource Locator"** or **"Universal Resource Locator"** or **"URL"** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be

specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

m. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computer Encryption

11. Encryption is the process of taking plain text and scrambling it into an unreadable format called "cipher text". This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the Internet. When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption. To unlock the message, both the sender and recipient have to use a "secret" encryption key – a collection of algorithms that scramble and unscramble data back to its readable format.

12. Various encryption software is currently available that can encrypt individual files, folders, volumes, or entire disks within a computer, as well as USB flash drives and files stored in the cloud. There are two main methods of encryption: symmetric encryption, which involves securing data with a single private key, and asymmetric encryption, which uses a combination of multiple keys that are both public and private.

13. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize encryption on their computer and electronic media to protect their child pornography files from being discovered by their associates and law enforcement officers. When encryption is utilized by the subjects, law enforcement officers typically cannot access the encrypted containers without gaining access to the passwords.

NCMEC and Cyber Tipline Reports

14. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and

services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

15. As part of its functions, NCMEC administers the Cyber Tipline. The Cyber Tipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the Cyber Tipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the Cyber Tipline reports. These ICAC's review the Cyber Tipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

Cloud Storage

16. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations.

17. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:

a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

b. "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

c. "Cloud Service Provider" (CSP) is the entity that offers cloud computing services. CSP's offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual

machines, or Web hosting. Service is billed as a utility based on usage. CSP's maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP's reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a "remote computing service." CSP's may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

d. "Virtual Machine" (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

18. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers. The service is offered by Dropbox Inc., a company based in San Francisco, California.

19. Mega is a cloud storage and file hosting service offered by Mega Limited, an Auckland, New Zealand-based company. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.

20. Mega provides its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a "sharing link". A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means.

Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

21. Based on my training and experience, I know that individuals involved in child pornography offenses frequently store their child pornography files in cloud storage accounts such as Mega and Dropbox. I also know, based on my training and experience, that individuals often trade child pornography files by sending sharing links to their cloud storage accounts.

Verizon Location Records and Cloud Data

22. Verizon provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

23. Verizon allows customers to back up and store the contents of their cellular telephones and tablets to a Verizon Cloud. Contents that can be backed up to the Verizon Cloud include messages, images, videos, documents, contacts, and call logs. The Verizon Cloud allows users to wirelessly back up and synch contents between their cellular telephones, tablets, computers, and other devices.

24. Synchronoss Technologies Inc. is a software services company that provides digital, cloud, messaging, and Internet of Things (IoT) platforms to various companies. Verizon has a contract with Synchronoss Technologies Inc. to power, administer, and maintain the Verizon Cloud. Synchronoss Technologies maintains the contents of the Verizon Cloud accounts. However, Verizon maintains subscriber information, transactional records, and location information for the telephone accounts.

Other Social Media Applications

25. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

26. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation, a company based in Redmond, Washington.

27. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

28. Skype has a feature that provides its users with the ability to exchange Private Conversations. This Private Conversations feature allows users to have end-to-end encrypted audio calls and to exchange end-to-end encrypted text messages, images, videos, and audio files. The contents of these conversations are hidden in the chat notifications in order to keep the information that users share private.

29. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.

30. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.

31. Kik is a cross-platform instant messenger application available on smartphones. The application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content. Each Kik user has an account name, which is unique to that user, as well as a profile name.

32. Wickr is an instant messenger application administered by Wickr Inc., a company based in San Francisco, California. The application allows users to exchange end-to-end encrypted and content-expiring messages, photographs, videos, and other file attachments.

33. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize various social media and messenger applications to trade child pornography files and to communicate with other offenders and victims.

FACTS SUPPORTING PROBABLE CAUSE

Information from Cooperating Witness

34. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as "Adult Male A". Adult Male A has pled guilty in the United States District

Court for the Southern District of Ohio to one count of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e). As part of his plea agreement, Adult Male A admitted that he had produced child pornography in 2019 and that he had viewed child pornography files depicting other children.

35. As part of the investigation, Adult Male A was interviewed on two occasions in March 2020 and May 2020. During these interviews, Adult Male A identified that he had received child pornography files from an individual who lived in Troy, Ohio. During the first interview, Adult Male A referred to this individual as "WILLIAM" and advised that WILLIAM's last name might be HITCHINGS or HIGGINS. During the second interview, Adult Male A advised that this individual's name was either "WILL HIGGINS" or "WILL HITCHINGS".

a. I know, based on my training and experience, that WILL is a common nickname for WILLIAM. It is common, in my experience, for individuals to transpose nicknames with true names.

b. Based on the information Adult Male A provided about the individual who sent him the child pornography, there is probable cause to believe that Adult Male A was referring to HITCHINGS.

36. During the first interview in March 2020, Adult Male A minimized his involvement in child pornography activities. He only admitted that he received and viewed child pornography on a limited number of occasions, and he denied that he produced child pornography. Below is a summary of information that Adult Male A provided about HITCHINGS during the first interview:

a. Adult Male A reported that he received at least one video depicting child pornography from HITCHINGS on a past occasion. HITCHINGS sent this video to Adult Male A via Telegram. Adult Male A acknowledged that there may have been additional occasions in which HITCHINGS sent him (Adult Male A) child pornography files.

b. Adult Male A stated that he did not want to get HITCHINGS in trouble, but that HITCHINGS was "into" child pornography.

c. Adult Male A had been to HITCHINGS' residence in the past. Adult Male A saw HITCHINGS view child pornography and bestiality files on a computer that was in HITCHINGS' residence.

d. HITCHINGS had a large rack of computers inside of his residence.

e. Adult Male A described HITCHINGS' residence as being on State Route 41 (also known as Main Street) near a school in Troy, Ohio.

37. Adult Male A was interviewed again in May 2020 pursuant to his arrest. During this interview, Adult Male A admitted that he had produced, received, and distributed child

pornography files. He also provided additional information about HITCHINGS during this interview. Below is a summary of information that Adult Male A provided about HITCHINGS during the second interview:

a. On the first occasion that Adult Male A was at HITCHINGS' residence, HITCHINGS took Adult Male A into the basement. HITCHINGS had a black rack of computers in the basement. HITCHINGS asked if Adult Male A wanted to see some "crazy" videos and then proceeded to show Adult Male A videos depicting bestiality and child pornography.

b. Over one year ago, HITCHINGS gave Adult Male A a desktop computer that was "packed" full of child pornography and adult pornography files. The pornography included children having sex with other children and animals. Adult Male A later destroyed the hard drive that was in this desktop computer.

c. HITCHINGS also at one time gave Adult Male A a laptop computer that contained child pornography files.

d. HITCHINGS previously told Adult Male A that there was good child pornography on Telegram.

e. Adult Male A again described HITCHINGS' residence as being on State Route 41 near a school and where the road curved. Adult Male A identified that HITCHINGS lived with his boyfriend, CHRIS (no last name provided), and HITCHINGS' mother.

38. It was noted that during both of the interviews of Adult Male A, he sometimes talked about how his deceased relatives and God spoke to him. However, Adult Male A provided information about his child pornography activities that was consistent with other information obtained pursuant to the investigation, including information provided by victims and cooperating witnesses, information obtained from Adult Male A's electronic accounts pursuant to search warrants, and other information obtained pursuant to the investigation. It is therefore reasonable to believe that the information Adult Male A provided about HITCHINGS is credible.

39. It was also noted that Adult Male A provided more information about his own child pornography activities as well as HITCHINGS' child pornography activities during the second interview (which was conducted pursuant to Adult Male A's arrest). Based on my training and experience, I know that it common for individuals to withhold information about their criminal activities when first contacted by law enforcement officers. Individuals often withhold such information as a means to protect themselves and their co-conspirators from criminal culpability. It is not uncommon for such individuals to be more truthful during subsequent interviews when they are faced with additional evidence and/or during interviews conducted after they have been arrested.

Cyber Tipline Report

40. As part of the investigation, I have learned that Synchronoss Technologies Inc. filed a report to NCMEC's Cyber Tipline on or around November 23, 2020, regarding approximately six suspected child pornography or child exploitation files located in a Verizon Cloud account associated with the **TARGET CELL PHONE**. Synchronoss Technologies Inc. provided these approximately six suspected child pornography or child exploitation files to NCMEC as part of its Cyber Tipline report.

41. NCMEC forwarded Synchronoss Technologies Inc.'s Cyber Tipline report, along with the suspected child pornography or child exploitation files, to me for further investigation. Based on my review of the files and my training and experience, I believe that approximately six of the files depict child pornography. By way of example, three of the files are described as follows:

a. a968ea8e58fa4b458ed2f98b600f626f_file1.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white male child who is lying on his back with his legs spread apart, exposing his nude genitals to the camera. What appears to be an adult white male (whose face is not captured in the image) appears to be urinating on the child.

b. a968ea8e58fa4b458ed2f98b600f626f_file2.jpg: The file in an image that depicts what appears to be a nude pre-pubescent white male child performing fellatio on what appears to be an adult white male (whose face is not captured in the image).

c. a968ea8e58fa4b458ed2f98b600f626f_file3.jpg: The file is an image that depicts what appears to be two nude pre-pubescent white male children who are standing next to each other. One child is touching the other child's penis.

Records Obtained Pursuant to Search Warrants and Subpoenas

42. On or around January 12, 2021, Synchronoss Technologies Inc. was served with a search warrant requesting the account contents of the Verizon Cloud account associated with the **TARGET CELL PHONE** (hereinafter referred to as the "SUBJECT VERIZON CLOUD ACCOUNT"). The account contents provided by Synchronoss Technologies Inc. in response to the search warrant included approximately seven documents, approximately 1,647 image files, and approximately 90 video files. Below is a summary of information noted regarding these files:

a. More than 450 of the image and video files depicted a male who appears to be HITCHINGS. These files included the following:

i. A number of the images and videos depicted HITCHINGS engaged in sexually explicit conduct. Some of the images and videos depicted HITCHINGS engaged in sexually explicit conduct with a dog.

ii. A number of the images and videos depicted HITCHINGS in what appears to be a basement. Numerous computer and electronic media (including computers, computer servers, computer hardware, and suspected surveillance systems) were depicted in the images and videos of HITCHINGS. HITCHINGS was depicted accessing these computer devices in some of the images and videos.

1. As noted above, Adult Male A reported that HITCHINGS had a large rack of computers in his basement.

iii. The EXIF data and metadata for the images and videos indicated that they were produced during the approximate time period of 2013 through 2020.

iv. The EXIF data indicated that the following devices were utilized to produce the images: a Motorola Moto z3 (the device associated with the **TARGET CELL PHONE**), a GoPro Hero 4, an LGE Nexus 4 cellular telephone, an LG Model LG-918 cellular telephone, a Kyocera Model E6830 cellular telephone, and nine different models of Samsung cellular telephones.

v. One image depicted HITCHINGS' Ohio driver's license.

b. One image depicted a screen print of what appears to be an order confirmation from an Internet-based purchase. This order confirmation listed HITCHINGS' name as the recipient along with the address of 924 East Main Street, Troy, Ohio (hereinafter referred to as the "SUBJECT PREMISES").

c. Approximately three images depicted three packages from the United States Postal Service and United Parcel Service, all of which were addressed to HITCHINGS at the SUBJECT PREMISES. Approximately one image depicted a Packing List for an order, with HITCHINGS' name and the SUBJECT PREMISES listed as the recipient of the items on the document.

d. In addition to the images and videos depicting HITCHINGS with computer devices, numerous other images and videos depicted computer and electronic media – including computers, computer servers, computer hardware, and surveillance systems. Some of the images depicted what appears to be monitoring screens for the surveillance cameras. Based on these images as well as other information obtained pursuant to the investigation, it appears that there were surveillance cameras that capture both the interior and exterior of HITCHINGS' residence, and that monitoring screens for these cameras were located both in the basement as well as the living room of the residence.

i. Based on my training and experience, I know that individuals involved in criminal activities often utilize surveillance cameras as a means to both protect their homes from thefts (such as thefts from other drug suppliers and

drug users) and to monitor their homes for any potential contact with law enforcement officers.

e. One image depicted what appears to be a screen print from an Internet website. This screen print listed the email address of w.hitchings@gmail.com.

f. Approximately eight of the images depicted what appears to be child pornography. Six of these files were the same as those reported in the Cyber Tipline report filed by Synchronoss Technologies Inc. (as detailed above). The other two files are described as follows:

i. Felixxx_134931EdF_koz.jpg: The file is an image that depicts what appears to be a nude toddler-aged male child. The child's legs are straddled, exposing his nude genitals and anus to the camera. It appears that the child's legs are bound to his arms with black tape. What appears to be an adult white male (whose face is not captured in the image) is pointing his penis toward (or possibly touching his penis to) the child's leg and penis.

ii. Felixxx_143309iCO_6598.jpg: The file is an image that depicts what appears to be a pre-pubescent white male child. The child is turned upside down over the lap of what appears to be an adult white male (whose face is not captured in the image). The child's pants are pulled down, exposing his nude genitals and anus to the camera. The adult male's hands are touching the child's legs and buttocks. The adult male's penis is exposed and pointed over the child's buttocks.

g. Approximately two of the images depicted what appears to be nude pre-pubescent male children.

h. At least approximately 22 of the images and videos depicted substances that, based on my training and experience, appear to be controlled substances. These files included the following:

i. Approximately 10 of the images and videos depicted a green leafy substance that appears consistent with marijuana. In one of the images, the substance was contained in a foil pan placed on a scale, with the scale showing a weight of 1.69 ounces.

ii. Approximately four of the images and videos depicted a crystal rocky substance that appears consistent with methamphetamine. One of these images depicted the crystal substance in a Tupperware container on a scale, with the scale showing a weight of 26.21 grams.

iii. Approximately five of the images and videos depicted a white rocky substance that appears consistent with crack cocaine or methamphetamine.

Approximately two of the images depicted the substance in bags on a scale, with the scale showing weights of 2.04 grams and 0.79 grams.

iv. Approximately three videos depicted an individual smoking a substance from a bong.

v. The EXIF data for the images identified that they were produced with a Motorola Moto z3 cellular telephone (the device associated with the **TARGET CELL PHONE**) during the approximate time period of August 1, 2019 through November 1, 2020. The background shown in some of the images and videos appears to match the background of the basement where HITCHINGS was captured in other images and videos (as detailed above).

i. One of the documents had a title on the first page of the following: "Dome Network Camera Quick Start Guide". This document provided instructions on how to use a dome surveillance camera. Another document was entitled "Family Fun". This document required a password to access it, and as such, could not be viewed.

43. Based on the information contained in the SUBJECT VERIZON CLOUD ACCOUNT as well as other information detailed in the Affidavit, it appears that HITCHINGS has had access to numerous computer devices. It also appears that HITCHINGS has had access to controlled substances. Based on my training and experience, the drug paraphernalia depicted in some of the images and videos (such as the scales and packaging materials) as well as the quantities and weights of some of the substances depicted in the images are consistent with someone who distributes controlled substances.

44. On or around January 12, 2021, Verizon was served with a search warrant requesting information associated with the **TARGET CELL PHONE** (including historical cell site records) for the time period of January 1, 2020 through January 12, 2021. Records received from Verizon in response to the search warrant included the following information:

a. The **TARGET CELL PHONE** was subscribed to CHRISTOPHER SWEENEY (hereinafter referred to as "SWEENEY") at the SUBJECT PREMISES. The contact person listed for the account was HITCHINGS. HITCHINGS' address was also listed as being the SUBJECT PREMISES.

i. Based on my training and experience, I know that individuals' telephone accounts may be subscribed to in other persons' names for a variety of reasons. One such reason could be that the individual has poor credit. Another reason could be that the person is on a "family plan" with a relative(s) or friend(s). Yet another reason could be to conceal the person's identity when the telephone account is being used in furtherance of illegal activities.

ii. As detailed above, Adult Male A identified that HITCHINGS resided with his boyfriend, whose first name was "CHRIS". Based on the investigation

conducted to-date, it appears that SWEENEY and HITCHINGS are involved in a romantic relationship.

b. The device that utilized the **TARGET CELL PHONE** was a Motorola Moto z3 cellular telephone.

c. The historical cell site records for the **TARGET CELL PHONE** identified that it was consistently in the area of the SUBJECT PREMISES, including during overnight hours.

d. The historical cell site records were compared to two of the dates associated with the photographs of marijuana that were recovered from the SUBJECT VERIZON CLOUD ACCOUNT (as detailed above). This comparison provided the following information:

i. The EXIF data for approximately four of the photographs of marijuana recovered from the SUBJECT VERIZON CLOUD ACCOUNT identified that the photographs were produced with a Motorola Moto z3 cellular telephone on or around April 17, 2020 between approximately 8:31 a.m. and 11:46 a.m. One of these images depicted the marijuana on a scale (showing a weight of 1.69 ounces) and three of the images depicted the marijuana in an aluminum container and/or bowl. The cell site records identified that the TARGET CELLL PHONE was in the area of the SUBJECT PREMISES before, during, and after this approximate time period.

ii. The EXIF data for approximately three of the photographs of marijuana recovered from the SUBJECT VERIZON CLOUD ACCOUNT identified that the photographs were produced with a Motorola Moto z3 cellular telephone on or around November 1, 2020 at approximately 8:07 p.m. The cell site records identified that the **TARGET CELL PHONE** was in the area of the SUBJECT PREMISES both before and after this approximate time – specifically, that it was in the area of the SUBJECT PREMISES at approximately 7:57 p.m. and 8:23 p.m.

iii. Based on the information detailed above, as well as other information associated with the photographs (i.e., the items depicted in the background of the photographs), it is reasonable to believe that the quantities of marijuana from the images detailed above were photographed inside the SUBJECT PREMISES.

45. As part of the investigation of Adult Male A, records were obtained from Facebook Inc. pursuant to a search warrant for his Facebook account. These records identified that Adult Male A had "blocked" another Facebook account containing a profile name of "WILLIAM HITCHINGS" and a user identification number of 100003978596185. On or around January 13, 2021, an administrative subpoena was served to Facebook Inc. requesting subscriber information for the Facebook account with the user identification number of

100003978596185, as well as logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:

a. The account was created on or around June 20, 2012 in the name of "WILLIAM HITCHINGS". The vanity name for the account was whitchings.

b. The email address associated with the account was hitchingsw@gmail.com. The telephone numbers associated with the account were the **TARGET CELL PHONE** and telephone number 305-587-8639.

c. The log of IP addresses identified that the two most common IP addresses utilized to access the account were 71.66.197.244 and 71.66.197.242. The account was accessed as recently as on or around January 11, 2021.

46. On or around January 14, 2021, an administrative subpoena was served to Google LLC requesting subscriber information for the w.hitchings@gmail.com Google account (the email address that appeared in one of the images recovered from the SUBJECT VERIZON CLOUD ACCOUNT), as well as logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:

a. The account was created on or around September 12, 2004 in the name of "WILLIAM HITCHINGS".

b. The alternate email address listed for the account was wenglebot@yahoo.com. The sign-in telephone number for the account as well as the recovery telephone number for the account were both listed as being the **TARGET CELL PHONE**.

i. Based on my training and experience, I know that many email providers such as Google LLC ask their users to provide alternate or recovery email addresses and telephone numbers when signing up for email accounts. The email providers send various notifications regarding the use of the users' email accounts to the alternate email addresses and telephone numbers to serve as security measures (i.e., to ensure that users' accounts have not been hacked or otherwise compromised). The email provider may also send to the user's alternate account a verification code that is needed to change a password to the user's account or complete another type of account maintenance.

c. The log of IP addresses identified that the two most common IP addresses utilized to access the account were 71.66.197.244 and 71.66.197.242 (the same IP addresses utilized to access the Facebook account associated with the email address hitchingsw@gmail.com and the vanity name of whitchings). The account was accessed as recently as on or around January 11, 2021.

47. Charter Communications was identified as the Internet Service Provider for the IP addresses of 71.66.197.244 and 71.66.197.242 (the IP addresses utilized to access the

w.hitchings@gmail.com Google account and the Facebook account associated with the email address hitchingsw@gmail.com and the vanity name of whitchings). On or around January 19, 2021, an administrative subpoena was served to Charter Communications requesting subscriber information for these IP addresses on a sample of two of the dates and times that they were utilized to access the w.hitchings@gmail.com Google account. Records received from Charter Communications in response to the subpoena identified that they were both subscribed to East Main Technologies Inc. at the SUBJECT PREMISES.

48. As part of the investigation, FBI investigators reviewed publicly available information on various social media websites and messenger applications for any possible accounts associated with the TARGET CELL PHONE and the email addresses w.hitchings@gmail.com, hitchingsw@gmail.com, and wenglebot@yahoo.com. Among other accounts, investigators located the following:

a. Google accounts were located that were associated with the email addresses **hitchingsw@gmail.com** and w.hitchings@gmail.com. The profile pictures for these two accounts depicted a white male who appears to be HITCHINGS.

b. Skype account was located that was associated with the email address w.hitchings@gmail.com. This Skype account contained a user name of "o0bc0o" and a profile name of "WILLIAM".

c. A Telegram account was located that was associated with the **TARGET CELL PHONE**. The account had a display name of "Bee Cee" and a user name of "o0bc0o" (the same user name as the Skype account listed above). The account was presently offline.

i. As detailed above, Adult Male A identified that he received one or more child pornography files from HITCHINGS via Telegram.

49. On or around January 20, 2021, Microsoft Corporation was served with a search warrant requesting information associated with the Skype account with the user name of o0bc0o and/or associated with the email address w.hitchings@gmail.com. Records received from Microsoft Corporation in response to the search warrant included the following information:

a. The account was created on or around June 24, 2015 in the name of "WILLIAM HITCHINGS". The account was associated with the email address w.hitchings@gmail.com.

b. The o0bc0o Skype account user exchanged hundreds of chat messages directly with other users (hereinafter referred to as "User Chats"). These User Chats included the exchange of text messages, image and video files, and live video calls (of which the content could not be provided by Microsoft Corporation). At least approximately 14 of the image and video files sent by the o0bc0o Skype account user depicted HITCHINGS.

c. The User Chats revealed that on or around February 16, 2020, the o0bc0o Skype account user exchanged messages with another user who will be referred to for purposes of this Affidavit as "Skype User-1". The o0bc0o Skype user and Skype User-1 discussed a website that promoted individuals who have a sexual fetish in gear, which they referred to as a gear fetish or "GF". During the exchange, the o0bc0o Skype user sent a picture of a server that was consistent with some of the pictures recovered from the SUBJECT VERIZON CLOUD ACCOUNT. The o0bc0o Skype user made comments indicating that this server had a large storage capacity that could host the gear fetish website. Below are excerpts from this chat:

o0bc0o:	idk if I said before, but I have the means to kickstart a site and host it free and clear of everyone else.
o0bc0o:	idk if gf domain is available, and the variations off gearfetish don't play out so well
o0bc0o:	*Sends image of a computer server*
o0bc0o:	this is growing. storage is now redundant at 100tb
Skype User-1:	Oh really?
o0bc0o:	two cables lines and a metro E leased line. I can literally recreate GF and handle the traffic.

i. Based on my training and experience, I know that 100 terabytes (TB) consists a very large amount of computer data. A typical hard drive in a laptop or computer is generally 500 gigabytes (GB) to two TB.

d. The User Chats revealed that during the approximate time period of March 16, 2019 through February 2, 2020, the o0bc0o Skype user exchanged messages with another user who will be referred to for purposes of this Affidavit at "Skype User-2". During their communications, they appeared to communicate about child pornography and drug activities. These communications included the following:

i. The o0bc0o Skype user and Skype User-2 made comments indicating that they also communicated with each other via the Telegram, Wickr, and Kik smartphone messenger applications. There were also times when Skype User-2 sent the o0bc0o Skype user sharing links to Mega accounts. Based on the context of the communications, it appeared that the o0bc0o Skype user and Skype User-2 may have also traded child pornography files with each other via Telegram, Wickr, Kik, and/or Mega sharing links. By way of example, on or around January 25, 2020, Skype User-2 sent the o0bc0o Skype user a sharing link to a Mega account. Skype User-2 thereafter stated the following: "Here to keep that cock hard, have you found any groups here wickr or kik try to find more pedos[1]".

1 Based on my training and experience, I know that "pedo" is a term to refer to a pedophile or an individual who has a sexual attraction to children.

ii. During the approximate time period of May 7, 2019 through May 9, 2019, the o0bc0o Skype user made comments indicating that administrators of the Mega cloud storage service had found child pornography files in his Mega account and closed the account. The o0bc0o Skype user talked about his fears that law enforcement officers would execute a search warrant at his residence, and he also expressed thoughts of committing suicide. The o0bc0o Skype user made comments indicating that he thought he had taken necessary precautions to prevent his accounts from being detected. The o0bc0o Skype user also made comments about how law enforcement officers would not find anything on his computer media if a search warrant was in fact executed at his residence. Furthermore, the o0bc0o Skype user talked about how law enforcement officers previously executed a search warrant on a prior residence and did not locate any evidence. Based on my training and experience, these comments are consistent with someone who stores child pornography files on a cloud service and/or a server and/or possesses devices that utilize encryption. Below are excerpts from these communications:

o0bc0o:	Mega flagged my account
o0bc0o:	I'm out of this forever my homey.
Skype User-2:	Which one?
o0bc0o:	It doesn't matter.
Skype User-2:	What
Skype User-2:	Don't leave me
Skype User-2:	Lol
Skype User-2:	Will Miss you after all those years
o0bc0o:	check all your shit
o0bc0o:	check it
o0bc0o:	methinks there are those among us…fucking with shit
Skype User-2:	What??
Skype User-2:	Your ok
o0bc0o:	no, I'm not ok
Skype User-2:	What's going on
Skype User-2:	You scare me like this
o0bc0o:	Mega account got flagged
o0bc0o:	gave me a warning by email
o0bc0o:	second email 3 days ago, I just found it.
o0bc0o:	DIDN'T KNOW THEY COULD LOOK AT YOUR ENCRYPTED STORAGE
Skype User-2:	Damn close it and delete
o0bc0o:	generic threat went out. They know who I am.
o0bc0o:	they have DIRECT connection between the account and a paypal!
o0bc0o:	But if they sent out an email saying warning, then…
o0bc0o:	the second email they deleted the account….hold on I'll fucking show you
o0bc0o:	*Sends partial excerpt from an email that appears to be from the Mega website, addressed to*

aaggll@yahoo.com. Below is an excerpt from this message:

"Recently you were sent an email advising that your account was found to contain copies of files that were reported to as being objectionable under Section 31(1)(A) of the New Zealand Films, Videos, and Publications Classification Act 1993. In particular, this relates to depictions of sexual conduct with or by children, or young persons (Section 3(3)(a)(iv)), which is an offense carrying potentially lengthy prison sentences in your jurisdiction."

Skype User-2:	Which account was it your cp account?
o0bc0o:	Yes.
o0bc0o:	The email says
o0bc0o:	WE DELETED IT
o0bc0o:	DONT DO IT AGAIN
o0bc0o:	DONT COME BACK TO MEGA
oObc0o:	I paid for premium service, that goes back to my name.
o0bc0o:	Now…would I get a heads up if they were about to raid me?
o0bc0o:	no, of course not.
o0bc0o:	and how expensive would it be to give me a week heads up to dump all physical anythings?
o0bc0o:	and THEN Raid me?
o0bc0o:	very unlikely. I'm not that interesting.
Skype User-2:	Have you deleted your account yet?
o0bc0o:	YUes
Skype User-2:	Fuck
o0bc0o:	but it doesn't mean it's not archived, on ice for someone to look at down the road
o0bc0o:	There's not data on any systems or disk I possess. If they raid me if they fuck with me, it'll be a pain in the ass, but ultimately yield a bunch of shit it would cost a fortune for them to hold me to charge wise.
o0bc0o:	sigh
Skype User-2:	Positive thinking
o0bc0o:	I thought I knew all the ins and outs.
o0bc0o:	I fucking know security
Skype User-2:	You will be fine
o0bc0o:	I don't know where I lapsed.
o0bc0o:	I might not
Skype User 2:	Exactly
Skype User 2:	Exactly
o0bc0o:	You see, this happened before, the attorney general in my parents home state…raided my childhook home
o0bc0o:	did I ever tell you this?
Skype User-2:	No

o0bc0o:	They raided a home that had been vacant for 2 years.
o0bc0o:	they raided looking for a single video download
o0bc0o:	ONE tagged download from emule or some shit.
o0bc0o:	ONE BY FILE NAME
Skype User-2:	When was that
o0bc0o:	years ago. The house was empty.
o0bc0o:	So they went down the street where my family had their new house
o0bc0o:	got a new warrant
Skype User-2:	Did they find you ,?
o0bc0o:	took all their shit. Had to give it back because theyere was nothing to find
	. . . . .
o0bc0o:	even if I turn out safe…and take every precaution…
Skype User-2:	Always
o0bc0o:	how the fuck will I know I can stop looking over my shoulder.
o0bc0o:	I fucking cant
o0bc0o:	I almost shot myself yesterday.
o0bc0o:	I almost blew my brains out
Skype User-2:	With drugs I hope
o0bc0o:	No, with a fucking nine mill.
Skype User-2:	Fuck no
o0bc0o:	Oh god I wanted to so bad.
Skype User-2:	Don't do that
o0bc0o:	so much to lose
Skype User-2:	A waist of a nice cock and body lol
o0bc0o:	Could be very real.
o0bc0o:	Not knowing if a bunch of armed men might show up ANY TIME for YEARS to come…
o0bc0o:	I will never sleep again.
o0bc0o:	And I've been carrying my firearm again.
Skype User-2:	Move to another state
o0bc0o:	doesn't work like that
o0bc0o:	They know where I am
	. . . . .
o0bc0o:	cops…federal agents…these people LIVE to kill people like me.
o0bc0o:	and child porn is what ANY good Christian police type will kill over.
	. . . . .
o0bc0o:	Everyone around here gets followed.
o0bc0o:	sometimes stopped, yes.
o0bc0o:	I should just start killing them
o0bc0o:	slam the brakes on and be like OMG OFFICER I DIDN'T SEE YOU THERE
o0bc0o:	a deer came across the road

o0bc0o:	and when he approaches the car
Skype User-2:	Don't do that you will be inside st least lots if boys to fuck
o0bc0o:	shotgun blast the pig in the face.
Skype User-2:	Messy
o0bc0o:	turns me the fuck on
o0bc0o:	I hate them
o0bc0o:	stealing my life.

iii. On or around January 19, 2020, the o0bc0o Skype user talked to Skype User-2 about his apparent sexual interest in the children of a man with whom he had a sexual relationship. These comments included the following:

o0bc0o:	an unexpected surprise. The boy I was fucking I thought gave me HIV, he's sort of here all the time now. Body looks like a cut 16 year old. Had a couple daughters and talks to me about wanting to fuck them, things of that nature. Very bi, very suggestible, does what I tell him to do.
o0bc0o:	Anyway, he's into it, so fresh files, very helpful in encouraging that behavior
	. . . . .
o0bc0o:	he doesn't seem to mind camming. Thought I'd take him into a cam session of pedos and make him represent me
Skype User-2:	Mmmm good fuck toy, you may get him knotted mm
o0bc0o:	I will teach him about k9
o0bc0o:	and if he has any kids, I'm going to get inside of them too.
o0bc0o:	he might be a connection to that world
o0bc0o:	*Emoticon*
Skype User-2:	Make sure you going to film that for me
Skype User-2:	All of it
o0bc0o:	yup

iv. On or around February 2, 2020, the o0bc0o Skype user made comments indicating that he was n possession of controlled substances. The o0bc0o Skype user also made comments indicating that he had shown child pornography to his "runner"[2]. Below are excerpts from this conversation:

Skype User-2:	What's happening any good porn
o0bc0o:	nah.
o0bc0o:	I got a TINY bit of drugs though.
Skype User-2:	Mmm so you getting high …nice

2 Based on my training and experience, I know that individuals involved in drug trafficking offenses use the term "runner" to refer to individuals who transport drugs for them.

o0bc0o:	*Sends image of a crystal-like substance that appears consistent with methamphetamine*
o0bc0o:	Two ounces
Skype User-2:	Mmm
Skype User-2:	Party time
o0bc0o:	All the time because it pretty much refills itself
o0bc0o:	I also made gummy bears
o0bc0o:	Anyone and everyone who eats one of them unavoidable becomes unconscious for 4 to 6 hours
Skype User-2:	Nice way to rape hehe
o0bc0o:	Like this stuff is stronger than valium or xanax
o0bc0o:	Yah
o0bc0o:	Def for rapes
o0bc0o:	Hehe
Skype User-2:	Nice any coming over
Skype User-2:	Who are the lucky ones to be used hehe
Skype User-2:	Lifeless fuck toy cum dump
o0bc0o:	*Sends video file depicting what appears to be HITCHINGS having anal intercourse with another male*
	. . . . .
Skype User-2:	Mmm nice which bitch is that
o0bc0o:	My runner.
o0bc0o:	He gets what I need
Skype User-2:	Your load lol
o0bc0o:	Hah among other things
o0bc0o:	He likes girls and guys.
o0bc0o:	Not so sure about boys
o0bc0o:	But I make him watch it.
Skype User-2:	Mmm horny what you show him
Skype User-2:	Hard fucking or just boys playing
o0bc0o:	Toddler. Rapey stuff.
o0bc0o:	Hsrd fucking or just bored is playing? When do I just watch them play? That's not good enough. I always watch them fuck.

Other Records

50. Based on review of a police report of the West Milton (Ohio) Police Department, I learned that on or around January 15, 2017, a police officer was dispatched to a residence in West Milton, Ohio. The occupant reported that his son had located an abandoned cellular telephone on a nearby street. This abandoned cellular telephone was turned over to the officer. The officer thereafter received a telephone call from HITCHINGS, who reported that he was the owner of the abandoned telephone. The officer requested that HITCHINGS provide proof that he was the owner of the telephone. A few weeks later, an officer released the telephone to HITCHINGS (although the report did not detail what proof, if any, that HITCHINGS provided that he was the owner of the telephone). HITCHINGS signed a

property receipt for the telephone. On this receipt, he identified that his telephone number was the **TARGET CELL PHONE**.

51. Records from the Ohio Bureau of Motor Vehicles identified that HITCHINGS utilized the SUBJECT PREMISES (the address associated with the **TARGET CELL PHONE**) on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles identified that a 2011 Chevrolet Tahoe (hereinafter referred to as the "SUBJECT VEHICLE") is registered to HITCHINGS at the SUBJECT PREMISES.

52. Records from the Ohio Bureau of Motor Vehicles identified that three other individuals utilized the SUBJECT PREMISES on their current Ohio driver's licenses: SWEENEY, RYAN WESTENDORF (hereinafter referred to as "WESTENDORF"), and ANDREW BAKER (hereinafter referred to as "BAKER"). Records from the Miami County (Ohio) Auditor's website identified that SWEENEY presently owns the SUBJECT PREMISES.

Business Records

53. Records from the Ohio Secretary of State identified that SWEENEY registered two business trade names in 2013: Sweeney Communications and Clear Voice One. The registration paperwork identified that the business address for both businesses was the SUBJECT PREMISES. The paperwork identified that the general nature of the Sweeney Communications business was "Communications Equipment Sales and Service and Computer Network Sales and Service". The paperwork identified that the general nature of the Clear Voice One business was "VOIP Phone Systems". The trade name for Clear Voice One expired and was cancelled by the Secretary of State in 2018.

54. Records from the Ohio Secretary of State also identified that in 2013, SWEENEY filed Articles of Incorporation for a business with the name of East Main Technologies. SWEENEY was listed as the statutory agent for this business, and his address was listed as being the SUBJECT PREMISES.

55. As part of the investigation, I have accessed various Internet websites that provide information about businesses. One of these websites (www.buzzfile.com) identified that Sweeney Communications, which also operates under the name of Clear Voice One, operates in the local and long distance telephone communications business. Another website (www.zoominfo.com) identified that Clear Voice One provides low cost Voice Over Internet Protocol (VOIP) phone services to businesses and residences.

56. A website was located for what appeared to be SWEENEY's Clear Voice One business at www.clearvoice1.com. However, this website is not currently operational. A Facebook social media account was located for Clear Voice One, but there were not any public postings to this account since 2017. No websites were located for Sweeney Communications.

57. An operational website was located for East Main Technologies at www.eastmaintech.com. According to this website, the company provides various computer services to businesses and residences, such as network monitoring, cloud backup, peripheral support, anti-virus

protection, workstations, and other management of servers. A Facebook account was also located for East Main Technologies.

58. Social media accounts were located on the publicly available information of the Facebook, Instagram, and Twitter websites that appear to be utilized by SWEENEY. Postings were found on these websites indicating that SWEENEY was employed at Walmart. No recent postings were found indicating that SWEENEY worked at or operated East Main Technologies, Clear Voice One, or Sweeney Communications.

59. A social media account was located on the publicly available information of the Facebook website that appeared to be utilized by WESTENDORF. The profile page for the account indicated that WESTENDORF was employed in Client/Vendor Relations, Systems Support, and "Dog Mother" for East Main Technologies as well as in Sales, Technical Support, and Graphic Design for Clear Voice One.

60. The publicly available information of the Facebook account with the vanity name of whitchings was located and reviewed. No information was located on this account indicating that HITCHINGS worked or operated East Main Technologies, Clear Voice One, or Sweeney Communications.

61. As part of the investigation, an FBI Task Force Officer contacted the City of Troy (Ohio) Income Tax Department. A representative from the Income Tax Department provided the following information:

a. The City of Troy Income Tax Department has not received any business income tax returns for Clear Voice One, Sweeney Communications, or East Main Technologies. It should be noted that business tax returns are not required for businesses if they are operated by sole owners. In such cases, the owner is required to report his/her business income on a Schedule C of his/her federal returns. The City of Troy requests that the Schedule C's be attached to the city returns.

b. The City of Troy Income Tax Department has received personal tax returns from SWEENEY. His 2019 return identified that he had a business loss of approximately $7,000. However, his Schedule C did not identify the name or type of business that generated this loss. Returns that the City of Troy Income Tax Department received from SWEENEY prior to 2019 did not include any Schedule C forms, indicating that he did not have any business income or losses.

c. The City of Troy Income Tax Department has not received any personal tax returns for HITCHINGS or WESTENDORF in any previous tax years.

62. Based on the information detailed above, some of the computer servers depicted in the images and videos recovered from the SUBJECT VERIZON CLOUD ACCOUNT could be related to the current or historical operation of the Clear Voice One, Sweeney Communications, and/or East Main Technologies businesses. However, based on the information detailed above, these businesses either do not appear to be currently operational and/or do not appear to be generating any profits or significant income.

63. Based on the images and videos recovered from the SUBJECT VERIZON CLOUD ACCOUNT and the o0bc0o Skype account, it appears that HITCHINGS regularly uses computer equipment (including the servers) located in the basement of the SUBJECT PREMISES. No images were recovered from the SUBJECT VERIZON CLOUD account that depicted SWEENEY using the computer equipment in the basement. As detailed above, the user of the o0bc0o Skype account talked about using his server to operate a website that promotes individuals having a sexual fetish in gear. Also as detailed above, the user of the o0bc0o Skype account made comments consistent with someone who maintains child pornography files on cloud accounts and/or servers. Furthermore, again as detailed above, Adult Male A reported that HITCHINGS utilized computer media in the basement of the SUBJECT PREMISES to show Adult Male A videos depicting child pornography and to download child pornography files onto a computer that was given to Adult Male A.

64. Based on the information detailed above, HITCHINGS appears to be the primary user of the computer and electronic media located in the basement of the SUBJECT PREMISES. HITCHINGS does not appear to have any association with the operation of SWEENEY's businesses. Based on all of the information detailed in the Affidavit, there is probable cause to believe that the computer and electronic media located in the basement of the SUBJECT PREMISES contain evidence of HITCHINGS' child pornography activities.

Surveillance Activities

65. An FBI Task Force Officer and I have driven by the SUBJECT PREMISES on a number of occasions. During these times, the following was noted:

a. The location of the SUBJECT PREMISES is consistent with the description provided by Adult Male A of HITCHINGS' residence.

b. The SUBJECT VEHICLE has been consistently parked in the driveway of the SUBJECT PREMISES, as recently as on or around February 2, 2021.

c. A vehicle registered to SWEENEY has also been parked in the driveway of the SUBJECT PREMISES on several occasions. A vehicle registered to BAKER has not been seen at the SUBJECT PREMISES on any occasions.

d. There are a number of surveillance cameras attached to the **SUBJECT RESIDENCE** that appear to capture all sides of the residence.

Conclusion Regarding Use of Accounts

66. Based on all of the information detailed in the Affidavit, there is probable cause to believe that HITCHINGS is the user of the following:

a. The **TARGET CELL PHONE** and the SUBJECT VERIZON CLOUD ACCOUNT;

b. The email addresses w.hitchings@gmail.com, **hitchingsw@gmail.com**, and wenglebot@yahoo.com;

c. The Facebook account associated with the email address **hitchingsw@gmail.com** and the vanity name of **whitchings**; and

d. The o0bc0o Skype account.

67. Also based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:

a. HITCHINGS has used computer devices (including the **TARGET CELL PHONE** and other computer and electronic media located at the SUBJECT PREMISES) to possess, receive, and distribute child pornography files.

b. HITCHINGS has possessed controlled substances.

Cellular Telephone Location Information

68. In my training and experience, I have learned that Verizon is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

69. Based on my training and experience, I know that Verizon can collect E-911 Phase II data about the location of the **TARGET CELL PHONE**, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on Verizon's network or with such other reference points as may be reasonably available. I also know that Verizon collects Range to Tower (RTT) data. This data captures the time it takes for a signal to travel from the tower to the handset and back again. Based on this time, the network will provide a distance between the tower and cell phone.

70. Based on my training and experience, I know that location information from cellular telephones can be materially relevant in investigations involving child exploitation and drug offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims and co-conspirators. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location

information can lead to the identification of the places where computer devices used in furtherance of the crime may be present – including the **TARGET CELL PHONE.**

AUTHORIZATION REQUEST

71. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

72. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **TARGET CELL PHONE** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

73. I further request that the Court direct Verizon to disclose to the government any information described in Attachment B that is within the possession, custody, or control of Verizon. I also request that the Court direct Verizon to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with Verizon's services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on Verizon's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate Verizon for reasonable expenses incurred in furnishing such facilities or assistance.

74. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **TARGET CELL PHONE** outside of daytime hours.

75. I further request that the Court order that all papers in support of this application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 4th day of February 2021

ELIZABETH A. PRESTON DEAVERS
UNITED STATES MAGISTRATE JUDGE